

09/651,979
Art Unit 2137
Docket No. 8490

DISCUSSION

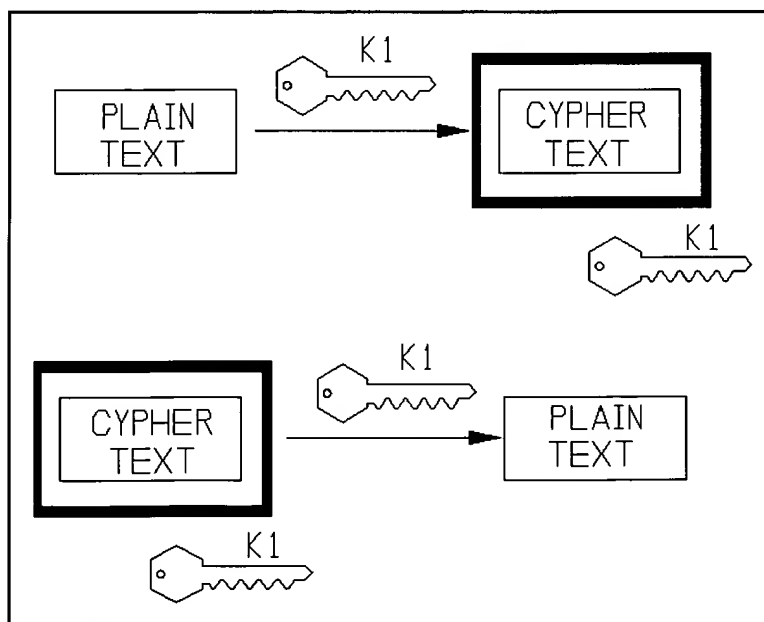
Applicant points out that all new claims state that an encryption key is derived from data which is stored in user-accessible memory or a portable computer. The applied references do not show that.

This Amendment will set forth, in simplified pictorial terms, one mode of operation of one form of the invention.

Sketch 1, below, illustrates conventions which will be used in this explanation. The top of the Sketch illustrates an encryption operation. PLAIN TEXT is encrypted into CYPHER TEXT using a key K1. The bold box around the CYPHER TEXT represents a lockbox, and the key at the lower right corner of the box indicates the key needed to de-crypt the CYPHER TEXT, that is, to "unlock" the lockbox and release the PLAIN TEXT from the lockbox.

The bottom of the Sketch indicates the converse operation. The encrypted CYPHER TEXT is de-crypted using key K1.

Of course, the system can be arranged so that a different key K2 (not shown), as opposed to K1, is needed to perform the de-cryption.



Sketch 1

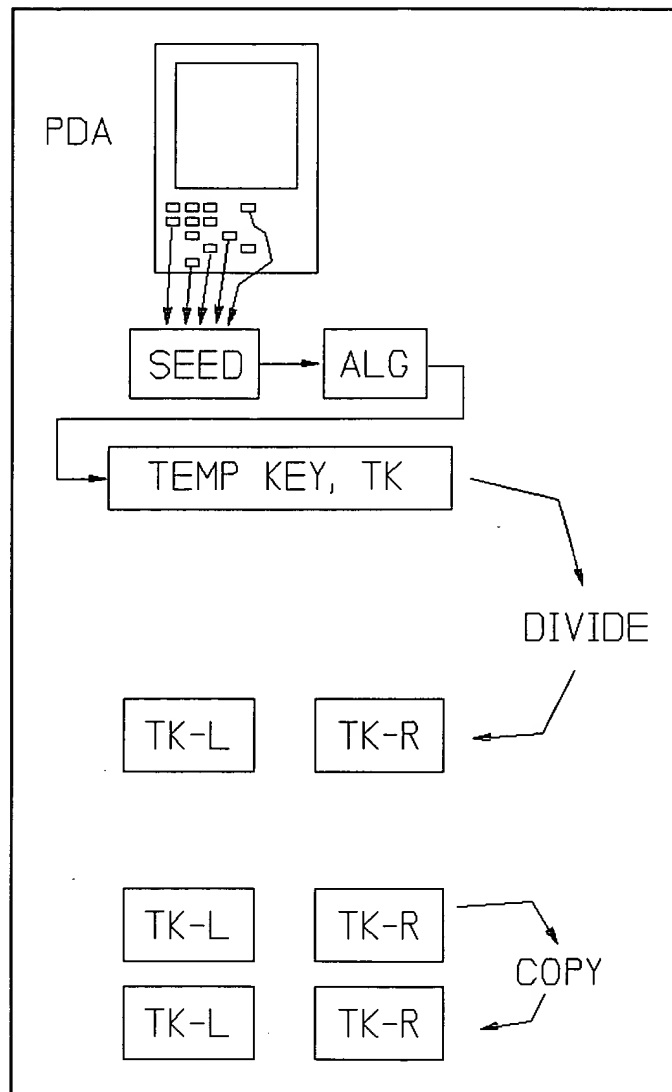
09/651,979
Art Unit 2137
Docket No. 8490

Sketch 2 illustrates processes undertaken by the PDA, Personal Digital Assistant. First, a SEED is created. This SEED is derived from data within the memory of the PDA. The rectangles represent the data. This data is not protected. Any user of the PDA can gain access to the data.

Applicant submits that this type of seed is contrary to conventional wisdom. Applicant submits that conventional wisdom teaches that the seed, and its origins, must be secret.

Next, an algorithm ALG creates a temporary key, TEMP KEY, or TK. Then TK is divided into two halves, left and right. Finally, the two halves are conceptually copied, producing two TK-L's (L: Left) and two TK-R's (R: Right).

09/651,979
Art Unit 2137
Docket No. 8490



Sketch 2

09/651,979
Art Unit 2137
Docket No. 8490

Sketch 3 illustrates further processing within the PDA. TK-R is used as a key to produce a session key SK from TK-L. The double arrow indicates that SK is symmetric, meaning that it can both encrypt and de-crypt data.

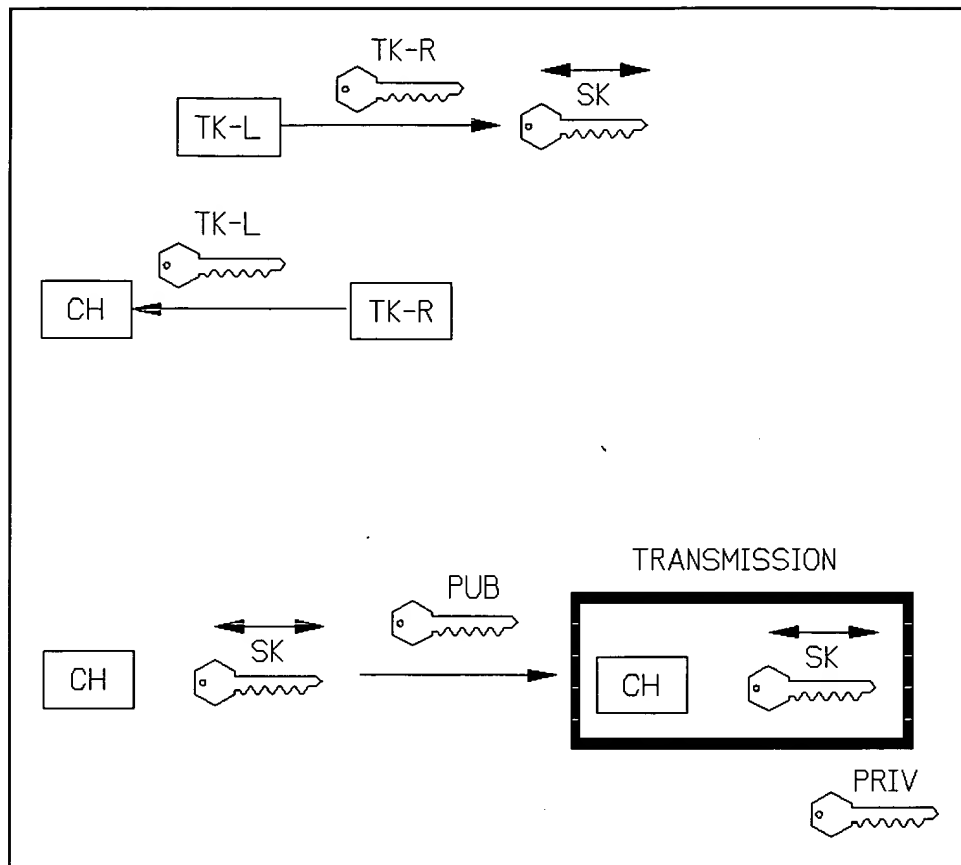
TK-L is used to encrypt TK-R, to produce a challenge CH.

(In general, a "challenge" is like a password-of-the-day for a clubhouse. You challenge people attempting to enter the clubhouse, by asking for the password. But the password will be different tomorrow.)

At the bottom of the Sketch, both the newly created CH and SK are encrypted using the public key PUB stored in the PDA. This produces what the Specification calls the TRANSMISSION. Note that a private key PRIV is needed to de-crypt the TRANSMISSION.

The public key PUB cannot be used for de-cryption, of course, because it is publicly available. If it could be used for the de-cryption, then the encryption would be pointless. Anybody could defeat the encryption by obtaining the publicly available public key.

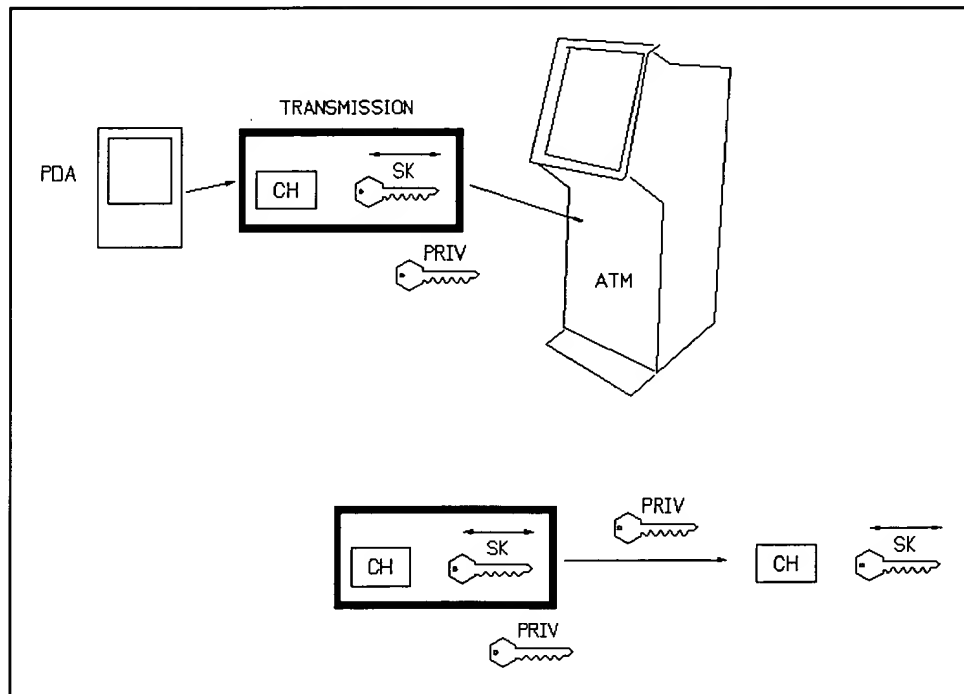
09/651,979
Art Unit 2137
Docket No. 8490



Sketch 3

09/651,979
Art Unit 2137
Docket No. 8490

Sketch 4, top, indicates that the PDA transmits the TRANSMISSION to a terminal, such as an ATM. Sketch 4, bottom, indicates that the ATM de-crypts the TRANSMISSION, using its private key PRIV, to recover the challenge CH and the session key SK.

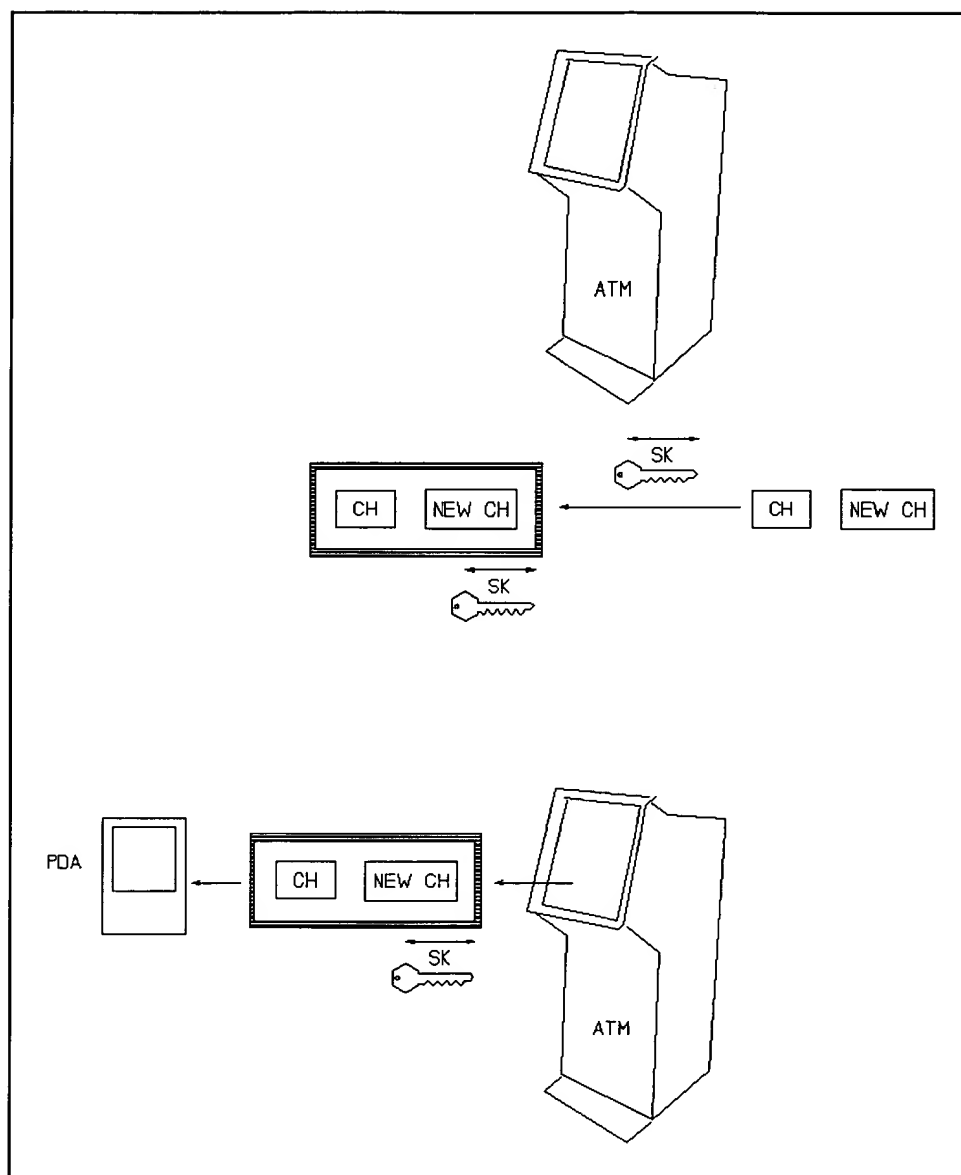


Sketch 4

09/651,979
Art Unit 2137
Docket No. 8490

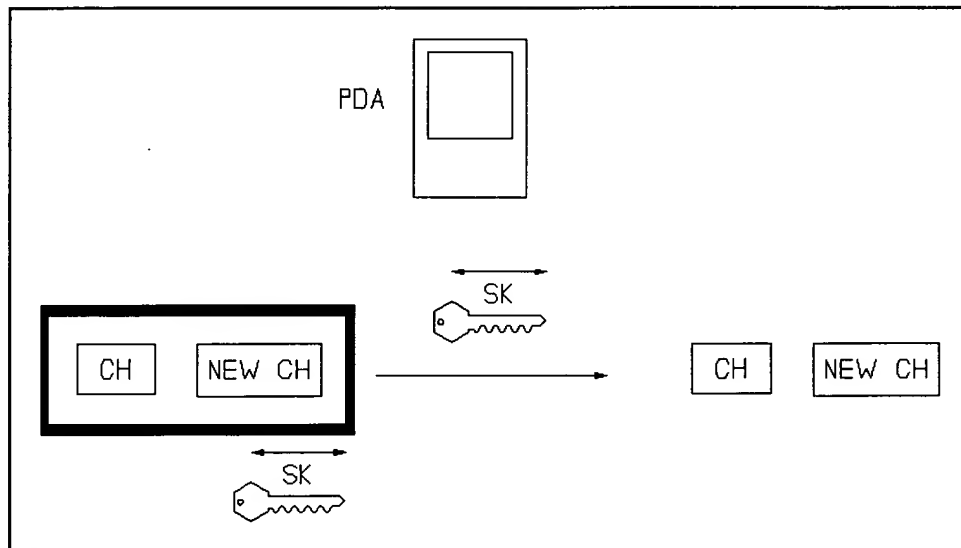
The ATM generates a new challenge NEW CH, based on the challenge CH received. Sketch 5, top, indicates that the ATM encrypts those elements, using the session key SK just received. Sketch 5, bottom, indicates that this encrypted data is transmitted to the PDA.

09/651,979
Art Unit 2137
Docket No. 8490



Sketch 5

Sketch 6 indicates that the PDA de-crypts the data, using the session key SK (created in Sketch 3, top), to recover the challenge CH and the new challenge NEW CH. The PDA can verify whether the ATM is a true ATM through the new challenge NEW CH. If the ATM is an imposter, the PDA can terminate the transaction.

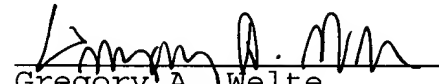


Sketch 6

Of course, some of these steps can be repeated. For example, the ATM can request a response to the new challenge NEW CH, to verify whether the PDA is genuine or an imposter.

09/651,979
Art Unit 2137
Docket No. 8490

Respectfully submitted,

A handwritten signature in black ink, appearing to read 'Gregory A. Welte', written over a horizontal line.

Gregory A. Welte
Reg. No. 30,434

NCR Corporation
1700 South Patterson Blvd.
WHQ - 4
Dayton, OH 45479
March 9, 2005
(937) 445 - 4956